DATA SHARING IN CLOUD STORAGE WITH KEY-AGGREGATE MODEL

Balukonda Sivakumar[1], Mr.K. Govardhan Reddy[2]
[1]*M.Tech student, CSE, Kottam college of Engineering, Chinnatekuru(V),Kurnool,Andhra Pradesh, India*
[2]*Associate Professor, CSE , Kottam college of Engineering, Chinnatekuru(V),Kurnool,Andhra Pradesh, India*

***Abstract*- Cloud storage is a storage of data online in cloud which is accessible from multiple and connected resources. Cloud storage can provide good accessibility and reliability, strong protection, disaster recovery, and lowest cost. Cloud storage having important functionality i.e. securely, efficiently, flexibly sharing data with others. New public–key encryption which is called as Key- aggregate cryptosystem (KAC) is introduced. Key-aggregate cryptosystem produce constant size ciphertexts such that efficient delegation of decryption rights for any set of ciphertext are possible. Any set of secret keys can be aggregated and make them as single key, which encompasses power of all the keys being aggregated. This aggregate key can be sent to the others for decryption of ciphertext set and remaining encrypted files outside the set are remains confidential.**

***Index Terms*- Double fed induction wind generators, direct power control, microgrid, robustsliding mode control, voltage regulation.**

I. INTRODUCTION

Cryptosystem is a pair of algorithm that take a key and convert plaintext to ciphertext and back. Cryptosystem is combination of three elements: keying information, operational procedure & encryption engine for the secure use. Cloud storage is a service where data is remotely maintain, managed and backup. Cloud storage is currently very popular. In enterprise we see demand of outsourcing of information. It is used as basic technology for very online services for private applications. In cloud computing things become worse due to share-tendancy. Privacy of data rely on the server to force access control after authentication which cause many times unexpected expose of the information. Information from different users can collected on seprate virtual machines but reside on single physical machine. Information from virtual machine can be easily get to another VM co-resident with target one. Cloud users do not have guarantee that cloud server can keep their information secure.

Sharing information is main task of cloud. For example, bloggers can want their personal photo , organization grant permission for this personal data. But problem is sharing of the encrypted data and effectiveness of that task. Take another example of dropbox for explanation. Alice can collect personal picture on dropbox and she thinks no one can watch her photos.

Due data loss possibility Alice does not feel secure and she encrypts all picture using own key before uploading. Another day her friend wants all pictures of the year in which bob appear. Alice use share option of dropbox but problem is that how to delegate decryption rights to bob. As increase in outsourcing of data the cloud computing serves does the management of data [1].

Its flexible and cost optimizing characteristic motivates the end user as well as enterprises to store the data on cloud. The insider attack is one of security concern which's needs to be focused. Cloud Service provider need to make sure whether audits are held for users who have physical access to the server. As cloud service provider stores the data of different users on same server it is possible that user's private data is leaked to others. The public auditing system of data storage security in cloud computing provides a privacy-preserving auditing protocol [2].

It is necessary to make sure that the data integrity without compromising the anonymity of the data user. To ensure the integrity the user can verify metadata on their data, upload and verify metadata [3].

Then there are 2 critical ways:
1.Alice encrypt whole picture with one encryption key and give secret key to bob.
2. Encrypt all picture with special key and send corresponding secret key to bob.

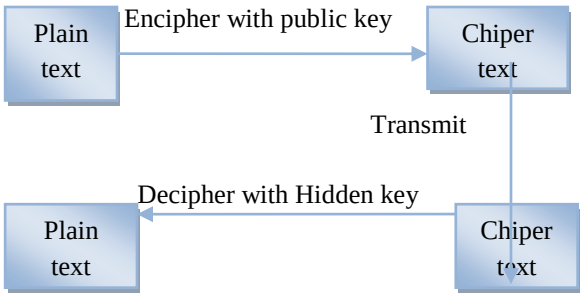

Fig. 1. Cryptosystem

II. RELATED WORKS

The flexible use of cloud storage for user is a need as it is seams accessing data locally though that is present at remote side. It is important to inspect the data set on the cloud. So it is necessary to allow a public audit for integrity of outsourced data through third party auditor (TPA). TPA is also beneficial for cloud service provider. It checks the correctness of the outsourced data. TPA should be able to do public auditability, storage correctness, privacy preserving, Batch auditing with minimum communication and computation overhead [2].

There are many cloud users who wants to upload there data without providing much personal details to other users. The anonymity of the user is to be preserved so that not to reveal the identity of data owner. Provable data possession (PDP) uses similar demonstrating marks to reduce computation on server, and network traffic. PDA ensures the data present on cloud which is un-trusted is original without accessing it. Security mediator (SEM) is approach allows the user to preserve the anonymity. Users are meant to upload all their data to SEM so that the SEM is not able to understand the data although it's going to generate the verification on data. As the users are signed at SEM it should not know the identity of uploader [3].

Another way for sharing encrypted data is Attribute-Based Encryption (ABE). It is likely to encrypt the data with attributes which are equivalent to users attribute rather than only encrypting each part of data. In ABE attributes description is considered as set so that only a particular key which is matched with attribute can decrypt the ciphertext. The user key and the attribute are matched if it matches it can decrypt a particular ciphertext. When there are k attributes are overlay among the ciphertext and a private key the decryption is granted [5].

A multi group key management accomplishes a hierarchical access control by applying an integrated key graph also handling the group keys for different users with multiple access authorities. Centralized key management plan uses tree structure to minimize the data processing, communication and storage overhead. It maintains things related to keying and also updates it. It accomplishes an integrated key graph for every user [6].

Identity-based encryption (IBE) is a vital primary thing of identity bases cryptography. The public key of user contains distinct information of user's identity. The key can be textual value or domain name, etc. IDE is used to deploy the public key infrastructure. The identity of the user is used as identity string for public key encryption. A trusted party called private key generator (PKG) in IBE which has the master secret key and gives secret key to users according to the user identity. The data owner collaborate the public value and the identity of user to encrypt the data. The ciphertext is decrypted using secret key [7].

In a multi attribute-authorities numbers of attributes are analyzed regarding the decryption key and the user must get a particular key related to the attribute while decrypting a message. The decryption keys are allocated independently to users those who have attribute identity without interaction between each other. Multi-authority attribute-based encryption allows real time deployment of attribute based privileges as different attributes are issued by different authorities. The attribute authorities ensure the honesty of the user privilege so the confidentiality is maintained by central authority [8].

III. PROPOSED SYSTEM

In modern cryptography, a basic problem we often study is about leveraging the secrecy of a small piece of knowledge into the ability to perform cryptographic functions (e.g. encryption,

authentication) multiple times. In this paper, we study how to make a decryption key more powerful in the sense that it allows decryption of multiple ciphertexts, without increasing its size.

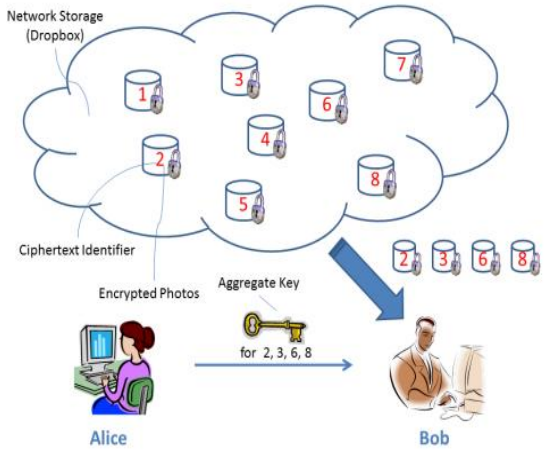

Fig. 2 . Alice shares files with identifiers 2, 3, 6 and 8 with Bob by sending him a single aggregate key.

A. KEY-AGGREGATE ENCRYPTION

A key aggregate encryption has five polynomial-time algorithms as

Setup Phase

The data owner executes the setup phase for an account on server which is not trusted. The setup algorithm only takes implicit security parameter.

Key Gen Phase

This phase is executed by data owner to generate the public or the master key pair (pk, msk).

Encrypt Phase

This phase is executed by anyone who wants to send the encrypted data. Encrypt (pk, m, i), the encryption algorithm takes input as public parameters pk, a message m, and I denoting ciphertext class. The algorithm encrypts message m and produces a ciphertext C such that only a user that has a set of attributes that satisfies the access structure is able to decrypt the message.

- Input= public key pk, an index i, and message m
- Output = ciphertext C.

Extract Phase

This is executed by the data owner for delegating the decrypting power for a certain set of ciphertext classes to a delegate.

- Input = master-secret key mk and a set S of indices corresponding to different classes.
- Outputs = aggregate key for set S denoted by kS.

Decrypt Phase

This is executed by the candidate who has the decryption authorities. Decrypt (kS, S, i, C), the decryption algorithm takes input as public parameters pk, a ciphertext C, I denoting ciphertext classes for a set S of attributes.

- Input = kS and the set S, where index i = ciphertextclass.
- Outputs = m if i element of S.

KAC in meant for the data sharing. The data owner can share the data in desired amount with confidentiality. KCA is easy and secure way to transfer the delegation authority. The aim of KCA is illustrated in Figure 2.

1) For sharing selected data on the server Alice first performs the Setup.
2) Later the public/master key pair (pk, mk) is generated by executing the KeyGen. The msk master key is kept secret and the public key pk and param are made public.
3) Anyone can encrypt the data m and this data is uploaded on server. With the decrypting authority the other users can access those data.
4) If Alice is wants to share a set S of her data with a friend Bob then she can perform the aggregate key KS for Bob by executing Extract (mk, S).
5) As kS is a constant size key and the key can be shared through secure e-mail. When the aggregate key has got Bob can download the data and access it.

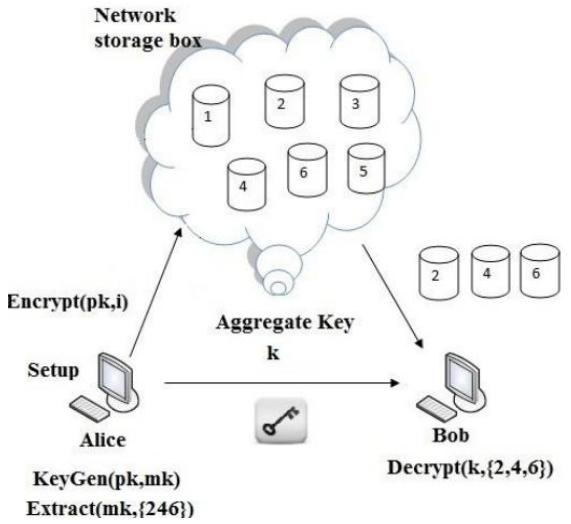

Fig 3 Use of KAC for data sharing

Advantages:-

- A decryption key is more powerful in the sense that it allows decryption of multiple cipher texts, without raising its size.
- The size of master-secret key, ciphertext, public-key, and aggregate key in our KAC schemes are all are kept constant size.
- KAC scheme is flexible in the sense that there is, no special relation is required between the classes.
- A canonical application of KAC is efficient data sharing scheme.
- The key aggregation property is especially useful when the delegation key to be efficient and flexible.
- The schemes enable a content provider to share her data in a confidential and selective way, with a fixed and small cipher text expansion, by distributing to each authorized user a single, compact,small aggregate key.
- The delegation of decryption can be efficiently implemented with the aggregate key.
- Number of cipher text classes is large.
- It is easy to key management.
- Particular Member can view their messages.
- We can provide rigorous security analysis, and extensive performance.

IV. CONCLUSION

With more mathematical tools, cryptographic schemes are getting more versatile and often involve multiple keys for a single application. In this article, we consider how to "compress" secret keys in public-key cryptosystems which support delegation of secret keys for different ciphertext classes in cloud storage. No matter which one among the power set of classes, the delegatee can always get an aggregate key of constant size. Our approach is more flexible than hierarchical key assignment which can only save spaces if all key-holders share a similar set of privileges.

REFERENCES

[1]. S. S. M. Chow, Y. J. He, L. C. K. Hui, and S.-M. Yiu, "SPICE - Simple Privacy-Preserving Identity-Management for Cloud Environment," in Applied Cryptography and Network Security – ACNS 2012, ser. LNCS, vol. 7341. Springer, 2012, pp. 526–543.

[2]. C. Wang, S. S. M. Chow, Q. Wang, K. Ren, and W.Lou, "Privacy-Preserving Public Auditing for Secure Cloud Storage," IEEE Trans.Computers, vol. 62, no. 2, pp. 362– 375, 2013.

[3]. B. Wang, S. S. M. Chow, M. Li, and H. Li, "Storing Shared Data on the Cloud via Security-Mediator," in International Conference on Distributed Computing Systems- ICDCS 2013. IEEE, 2013.

[4] D. Boneh, R. Canetti, S. Halevi, and J. Katz, "Chosen-Ciphertext Security from Identity-Based Encryption," SIAM Journal on Computing (SIAMCOMP), vol. 36, no. 5, pp. 1301–1328, 2007.

[5]. V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-Based Encryption for Fine-Grained Access Control of Encrypted data,"in Proceedings of the 13th ACM Conference on Computer and

Communications Security (CCS ’06). ACM, 2006, pp. 89–98.
[6]. Y. Sun and K. J. R. Liu, “Scalable Hierarchical Access Control in Secure Group Communications,” in Proceedings of the 23th IEEE International Conference on Computer Communications (INFOCOM ’04). IEEE, 2004.
[7]. D. Boneh and M. K. Franklin, “Identity-Based Encryption from the Weil Pairing,” in Proceedings of Advances in Cryptology – CRYPTO ’01, ser. LNCS, vol. 2139. Springer, 2001, pp. 213–229.
[8]. M. Chase and S. S. M. Chow, “Improving Privacy and Security in Multi-Authority Attribute-Based Encryption,” in CM Conference on Computer and Communications Security, 2009, pp. 121–130.

BIODATA

Author

Balukonda Sivakumar presently pursuing his M.Tech in CSE, Kottam College of Engineering, Chinnatekuru (V), Kurnool,Andhra Pradesh, India.

Co-Author

Mr.K. Govardhan Reddy received M.Tech. Presently working as Assistant Professor in Kottam College of Engineering,Chinnatekuru (V), Kurnool, Andhra Pradesh, India.